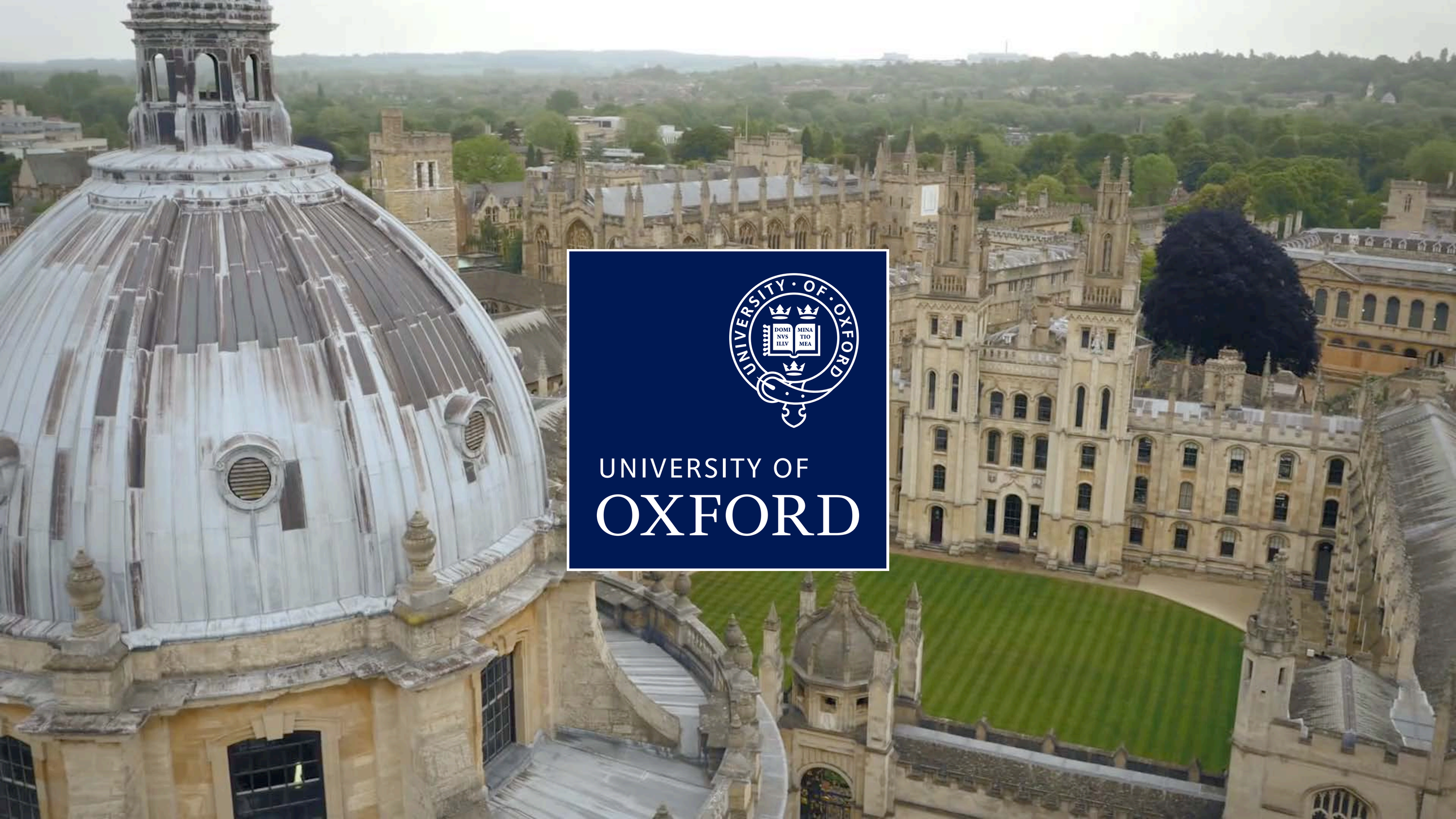

CLOUDSEC2019


UNIVERSITY OF
OXFORD

Oxford Research

- Oxford employs over 13,900 people, of which 7,260 are academics, researchers or teachers (56%).
- According to the 2014 Research Excellence Framework, the latest official UK-wide assessment of all university research, Oxford has the largest volume of world-leading research in the country.
- 5% of all the UK's graduate research students are studying at the University of Oxford.

Oxford researchers are major contributors to the global response to the Zika epidemic

Oxford Education

- Oxford was ranked first in the world in the Times Higher Education (THE) World University Rankings for 2017, 2018, 2019, and 2020.
- Nearly 24,000 students *(11,747 UG, 11,687 PG)*
- Oxford is very competitive: around 21,500 people applied for around 3,300 undergraduate places for entry in 2018.
- Oxford offers more than 300 different graduate degree programmes.
- 43% of our total student body – almost 10,000 students – are citizens of foreign countries. Students come to Oxford from over 150 countries and territories.

Oxford students celebrating at Radcliffe Camera Square after their final exams.

Oxford Information Technology

- Highly federated environment with 800 members of IT staff across over 110 units, plus 44 Colleges and Permanent Private Halls.
- Units operate largely independently
- Oxford operates one of the largest private networks in the country with
  - ~100,000 registered devices
  - redundant 40GBit/s Internet uplink

Oxford Cyber Security

UNIVERSITY OF OXFORD

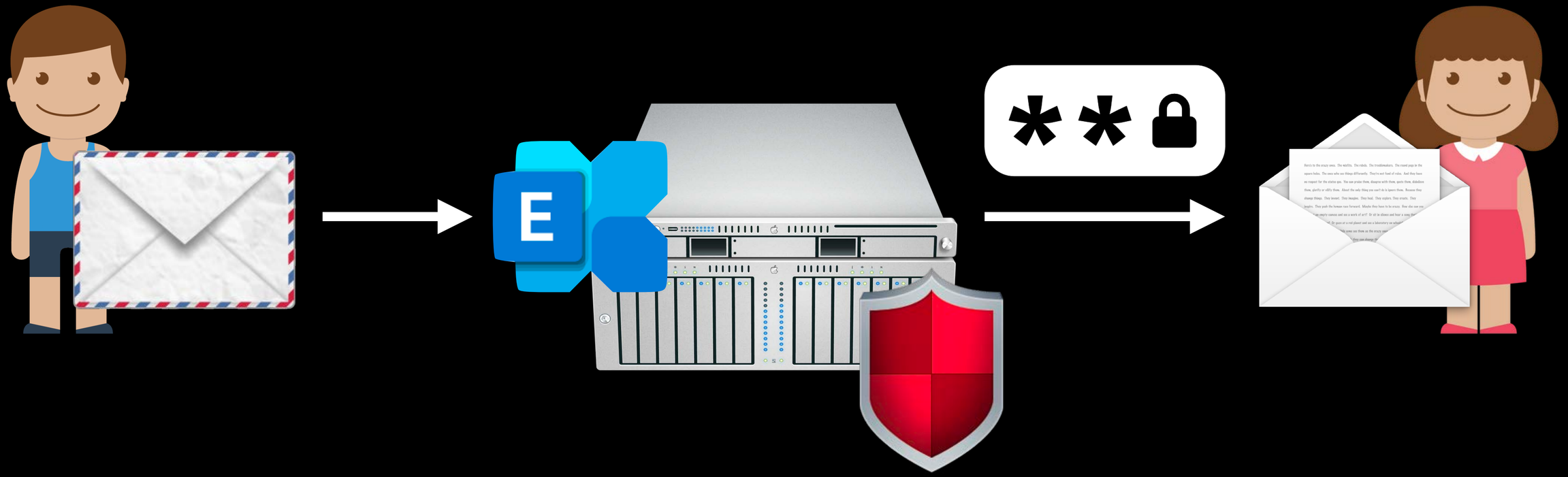
- 2019 marks the 25th anniversary of OxCERT.
- 17 security experts split across two teams cover all five functions: identify, protect, detect, respond, and recover.
- Offering services to the collegiate University similar to a managed security services provider.
- Collaboration with cyber security researchers.
- Deeply integrated in the international security community.

Threat Hunting

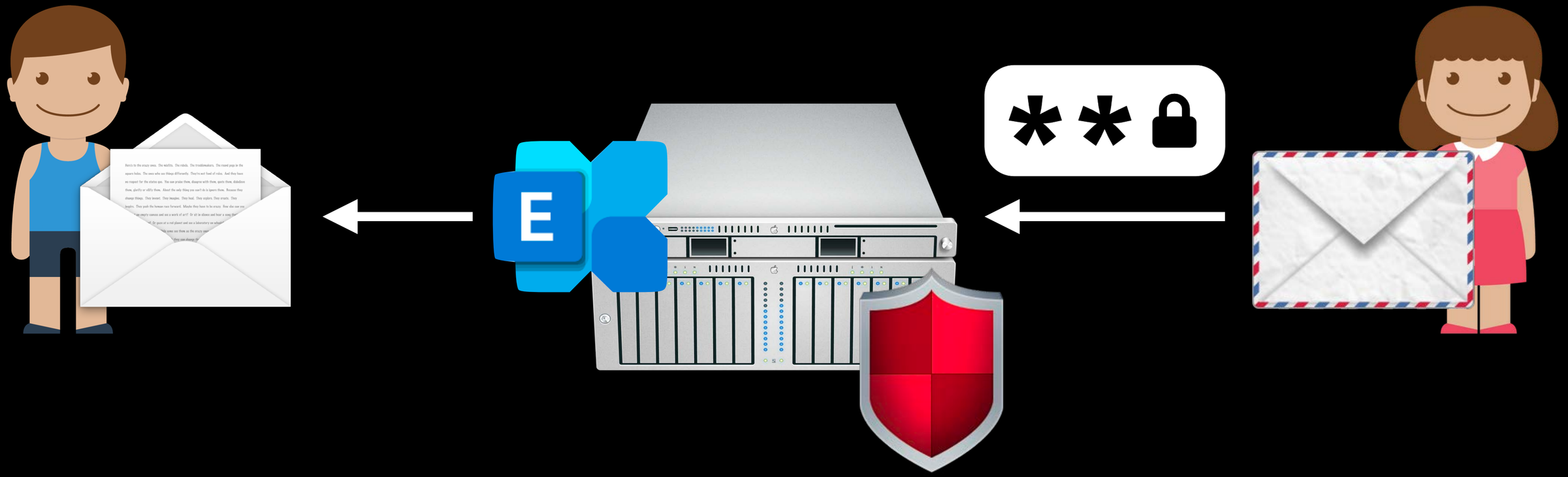
Lessons Learned from our Journey to the Cloud

Traditional Email Architecture

UNIVERSITY OF OXFORD



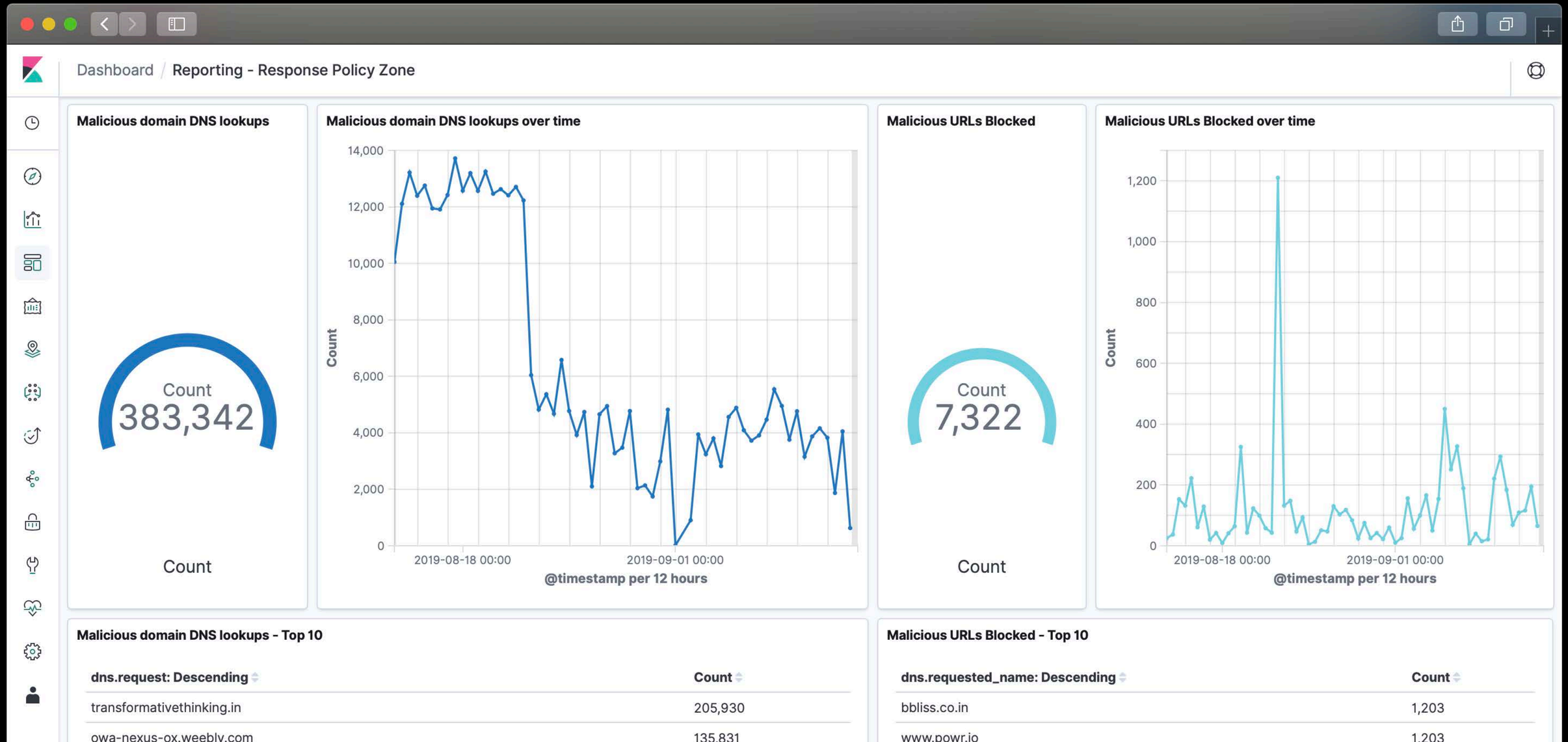
Traditional Email Architecture



UNIVERSITY OF
OXFORD

Reasons for a custom RPZ

UNIVERSITY OF OXFORD



Strategies against Phishing?

UNIVERSITY OF OXFORD

User education: training, awareness campaigns, internal phishing exercises.

Email security products.

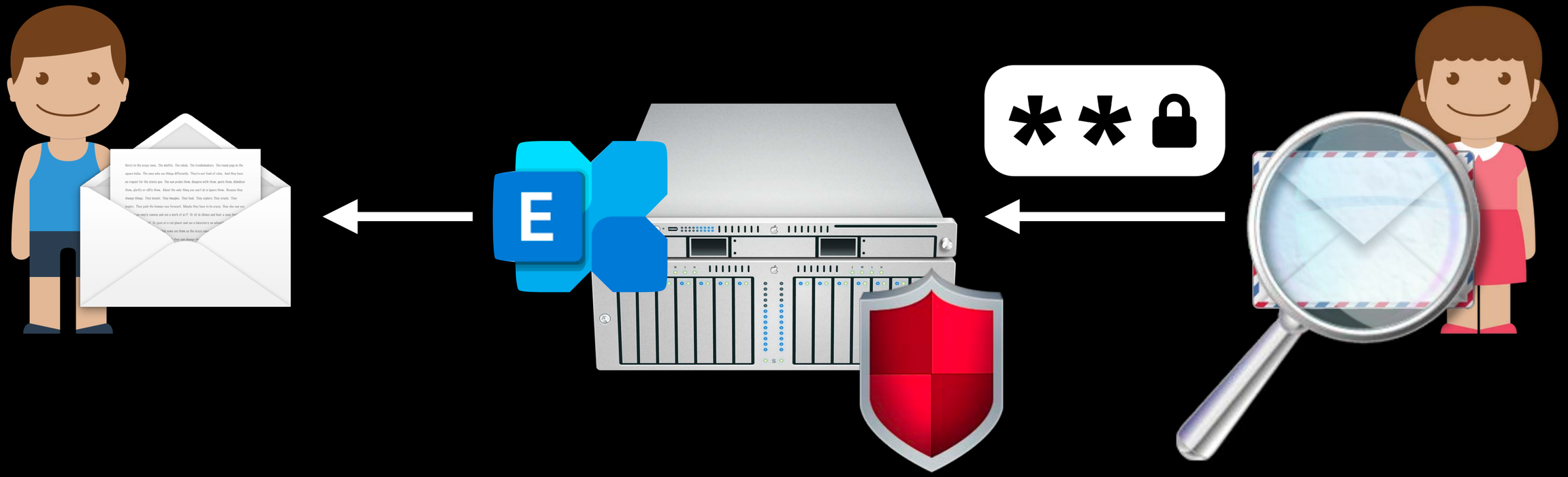
DNS Firewall (Response Policy Zone) to subvert phishing sites to a sinkhole.

Endpoint web filtering using the RPZ.

Compromised Accounts Behave Anomalously

Compromised Account Detection

UNIVERSITY OF OXFORD



Compromised Account Detection

UNIVERSITY OF OXFORD

detect_spammer.pl

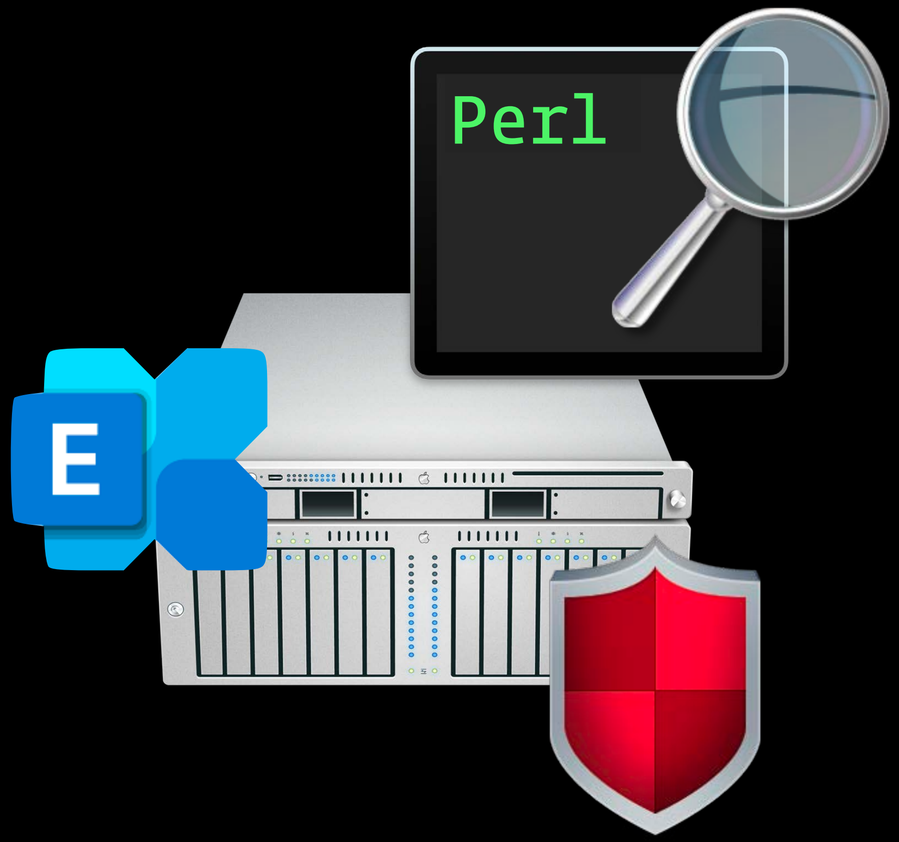
notify

```
1   #!/usr/bin/perl
2   # $HeadURL:
…   https://secret.oxcert.ox.ac.uk/svn/conf/rb3/systems/spam-detector.oxcert.ox.ac.uk/root/usr
…   /local/bin/detect_spammer.pl $
3   # $LastChangedRevision: 29666 $
4   # $LastChangedDate: 2019-06-13 14:21:07 +0100 (Thu, 13 Jun 2019) $
5   # $LastChangedBy: horst $
6   #
7   # *** Generated from sources/usr/local/bin/detect_spammer.pl.tt ***
8   #
9
10  use strict;
11  use warnings;
12  use Net::SMTP;
13  use Getopt::Long;
14  use vars qw($opt_help $opt_debug);
15  use Text::ParseWords;
16  use Switch;
17  use POSIX qw(strftime);
18
19  my $disabled_first = 10;
20  my $disabled_rate = 10;
21  my $mail_from='
22  my $mail_desc='OxCERT Email Spammer Alert ';
23  my $oxcert_email='
24  my @emails;
```

Compromised Account Detection

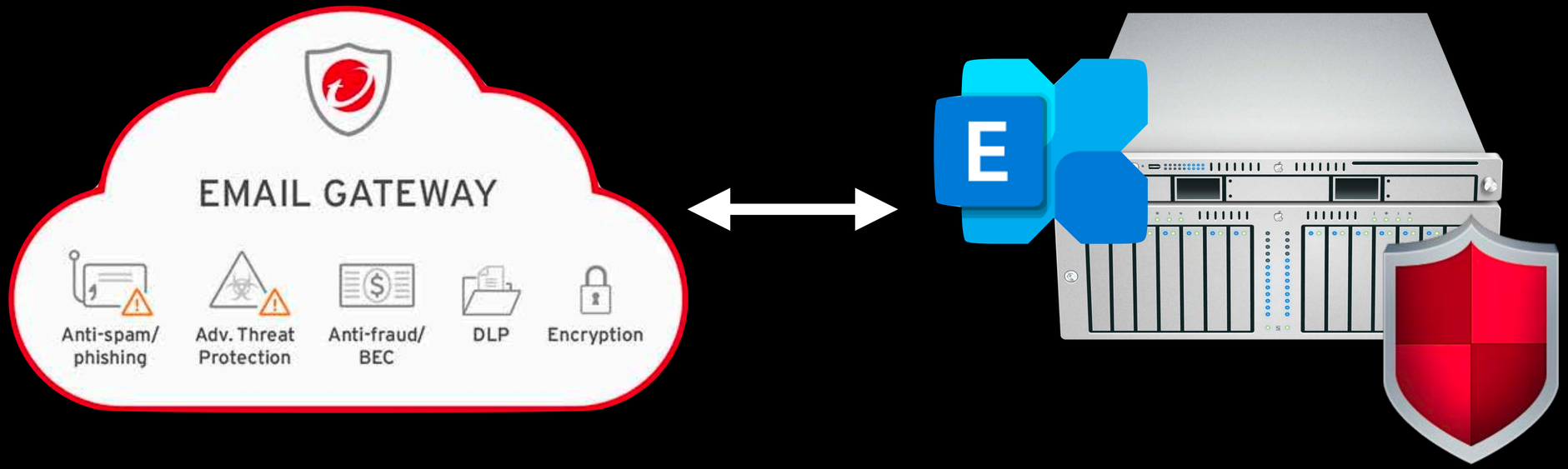

```
From: "OxCERT Email Spammer Alert" <detector@infosec.ox.ac.uk>
To: detections@infosec.ox.ac.uk
Subject: Possible Spammer alert - Rate limit exceeded: <help@it.ox.ac.uk>
Date: Fri, 13 Sep 2019 13:13:13 +0100

The following log entry was detected:

Sep 13 13:13:13 host exim[41679]: H=host.mail.ox.ac.uk [1.2.3.4]
X=TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256 CV=no F=<help@it.ox.ac.uk>
temporarily rejected RCPT <random@hotmail.com>: SND-FLD help@it.ox.ac.uk
sender address limit exceeded to random@hotmail.com rate=n+1 ratelimit=n

SSO username: user1234
FROM top subjects:
  (1298) Nexus Upgrade Message
```

UNIVERSITY OF OXFORD



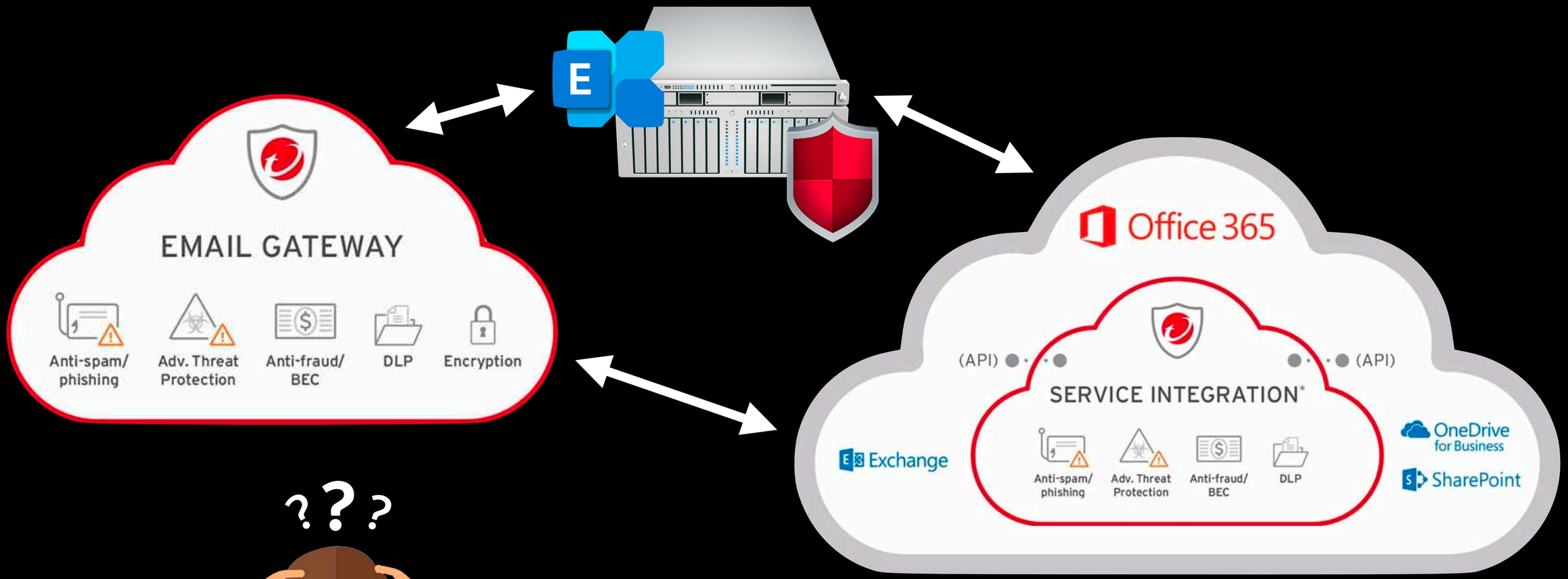
Email Security as a Service

UNIVERSITY OF OXFORD



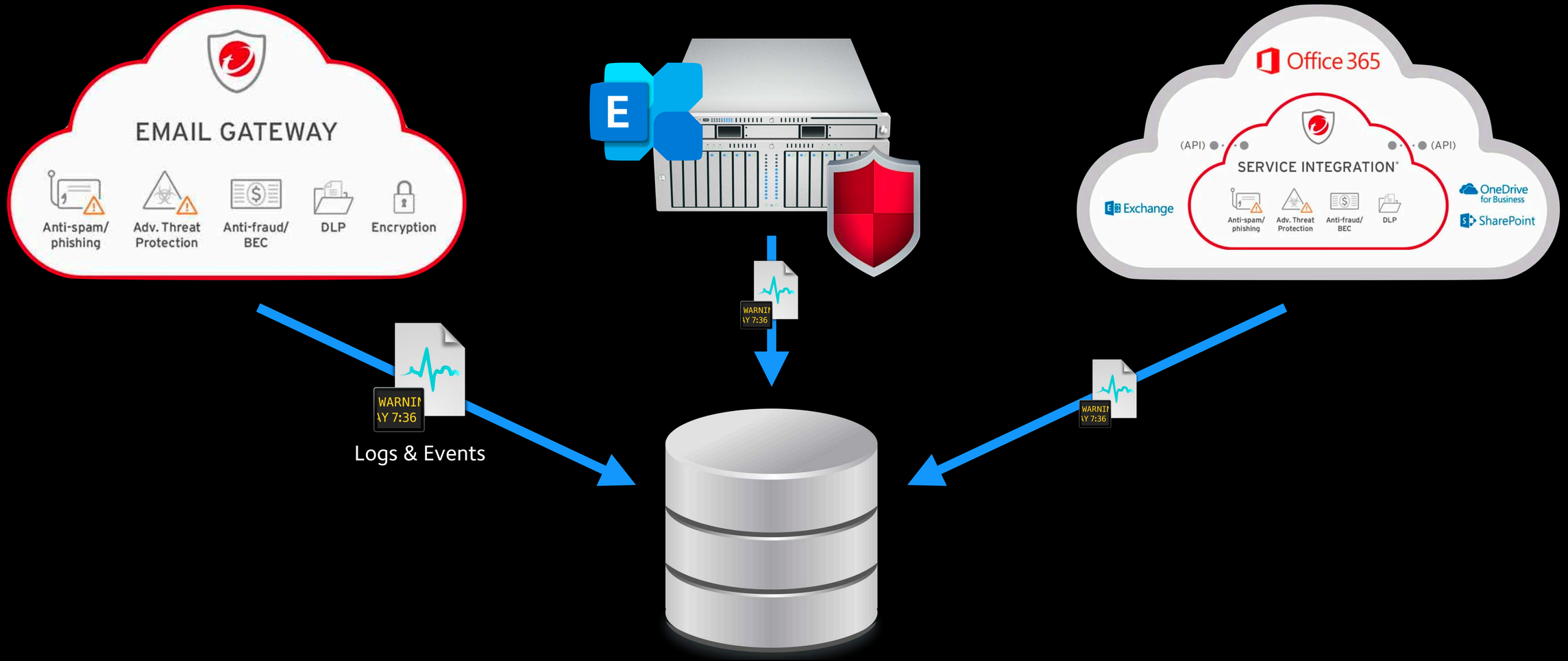
Hybrid Cloud

UNIVERSITY OF OXFORD



Hybrid Cloud Security Analytics

UNIVERSITY OF OXFORD



UNIVERSITY OF OXFORD

SIEM

Security Information and Event Management

UNIVERSITY OF OXFORD

SIEM+

Entity and User Behaviour Analytics

Security Orchestration, Automation and Response

Threat Intel Retro-Matching

The Tool Maketh the Team

UNIVERSITY OF OXFORD

SIEM+

SIRT

elastic

https://elastic.co

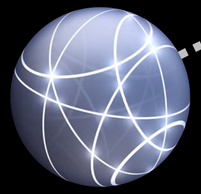
BEST PRACTICAL™

https://bestpractical.com/rtir/

The Tool Maketh the Team

UNIVERSITY OF OXFORD

Logs & Events



Network analysis

Assets & Compliance

SIEM+

Data storage
Data aggregation
Data correlation
Security analysis
Alerting
Reporting

Alerts & artefacts

Incident data

SIRT

Prioritisation
Workflow
Automation
Threat intelligence
Metadata & Search

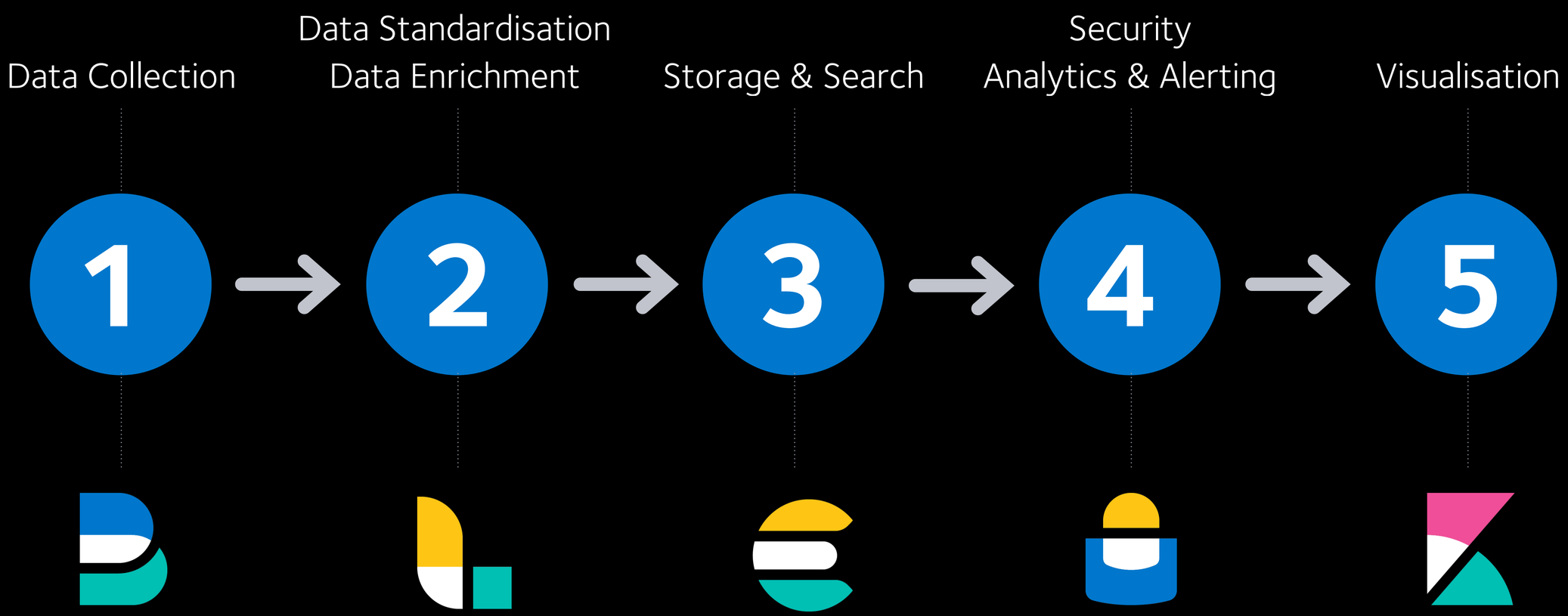
Incident Reports

Investigation

Countermeasures

Elastic Stack in a Nutshell

UNIVERSITY OF OXFORD



Get a Handle on Your Data

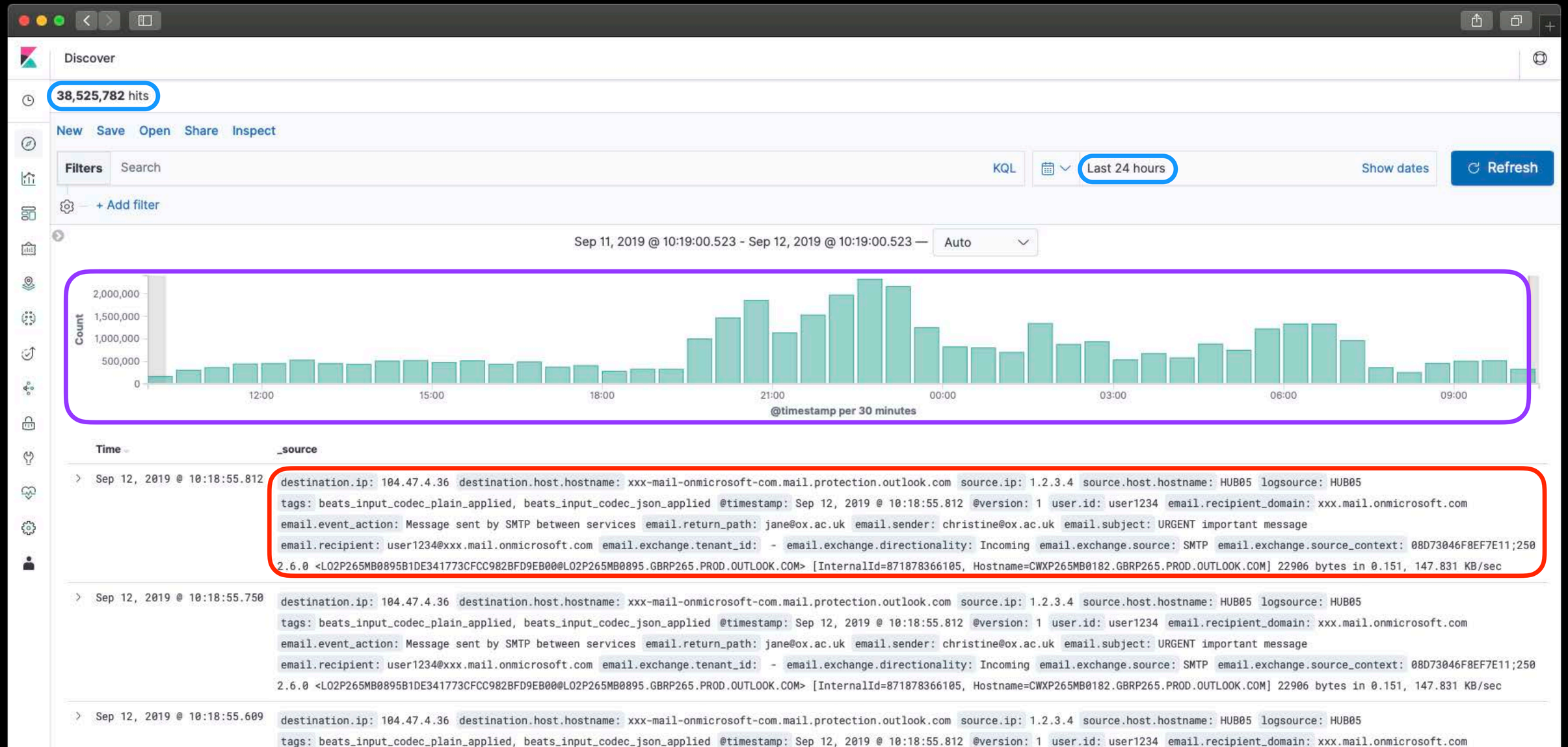
Just collecting all possible logs, events, and alarms does not help making sense out of them!

- NTP time source, UTC based logging, and ISO 8601 date
- Normalise your data during ingest

  e.g. `2001:420:1101:1::A` vs `2001:420:1101:1:0:0:0:a`
- Enrich during ingest and continuously curate metadata
- Use a consistent schema *(Elastic Common Schema)*
- Keep just the facts – filter and prepare your data

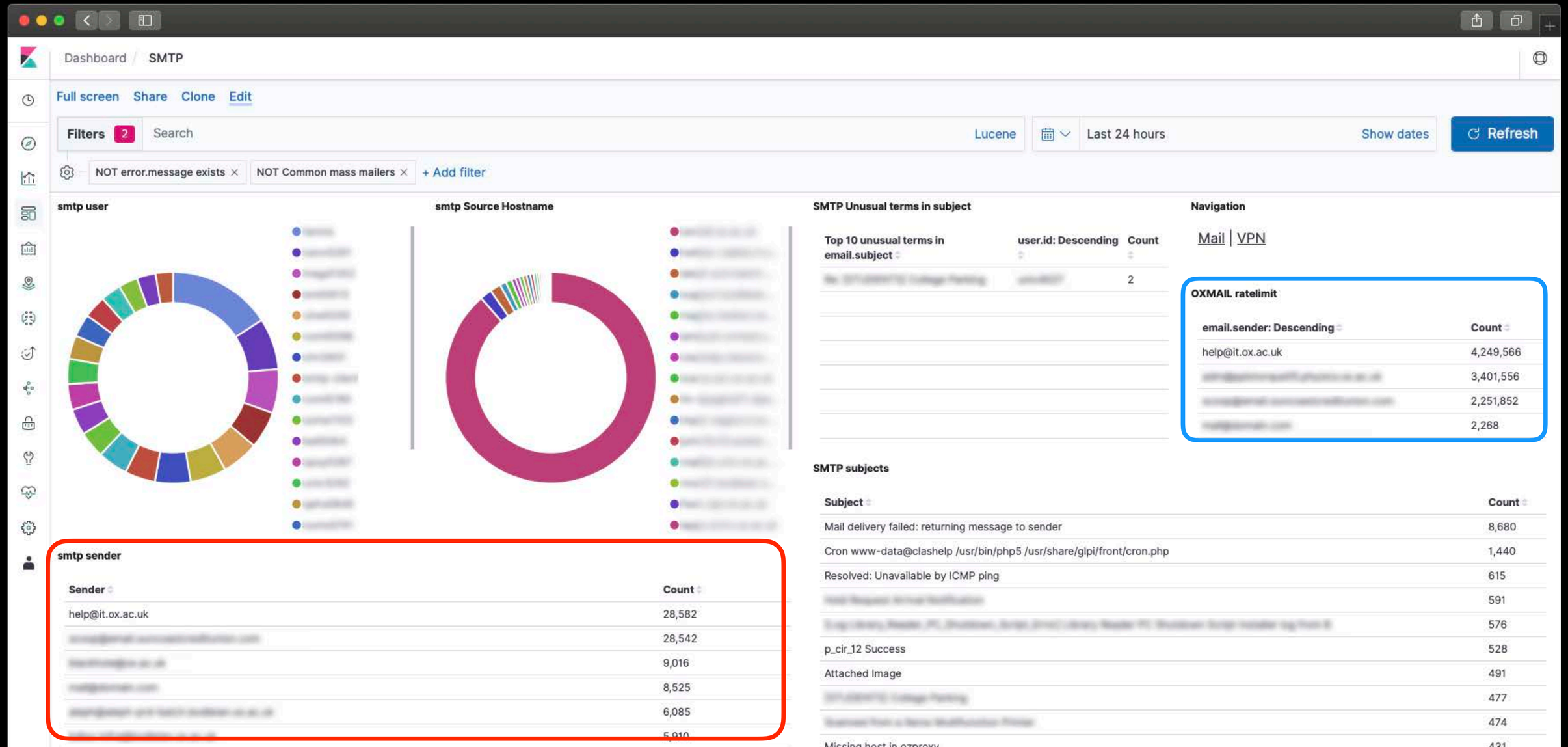
Data Discovery using Elastic

UNIVERSITY OF OXFORD



Dashboards using Elastic

UNIVERSITY OF OXFORD

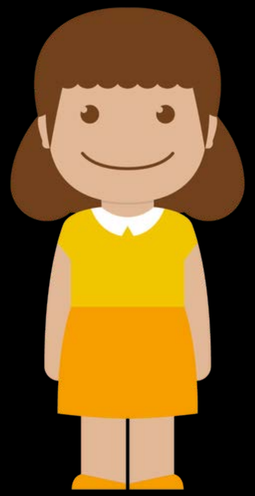


The Rise of the Machines

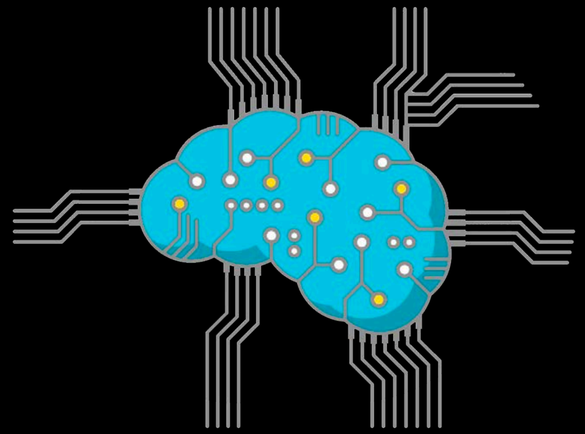
What is Machine Learning?

UNIVERSITY OF OXFORD

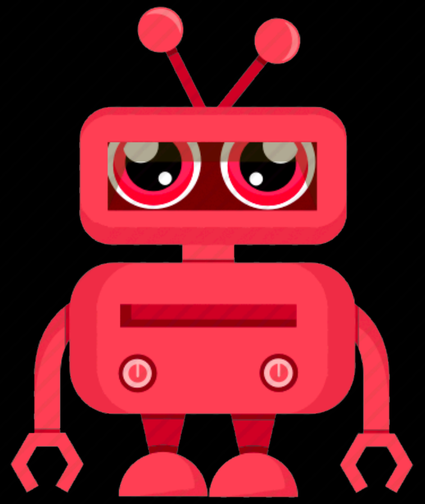
Learn from experience



Learn from ~~experience~~ data

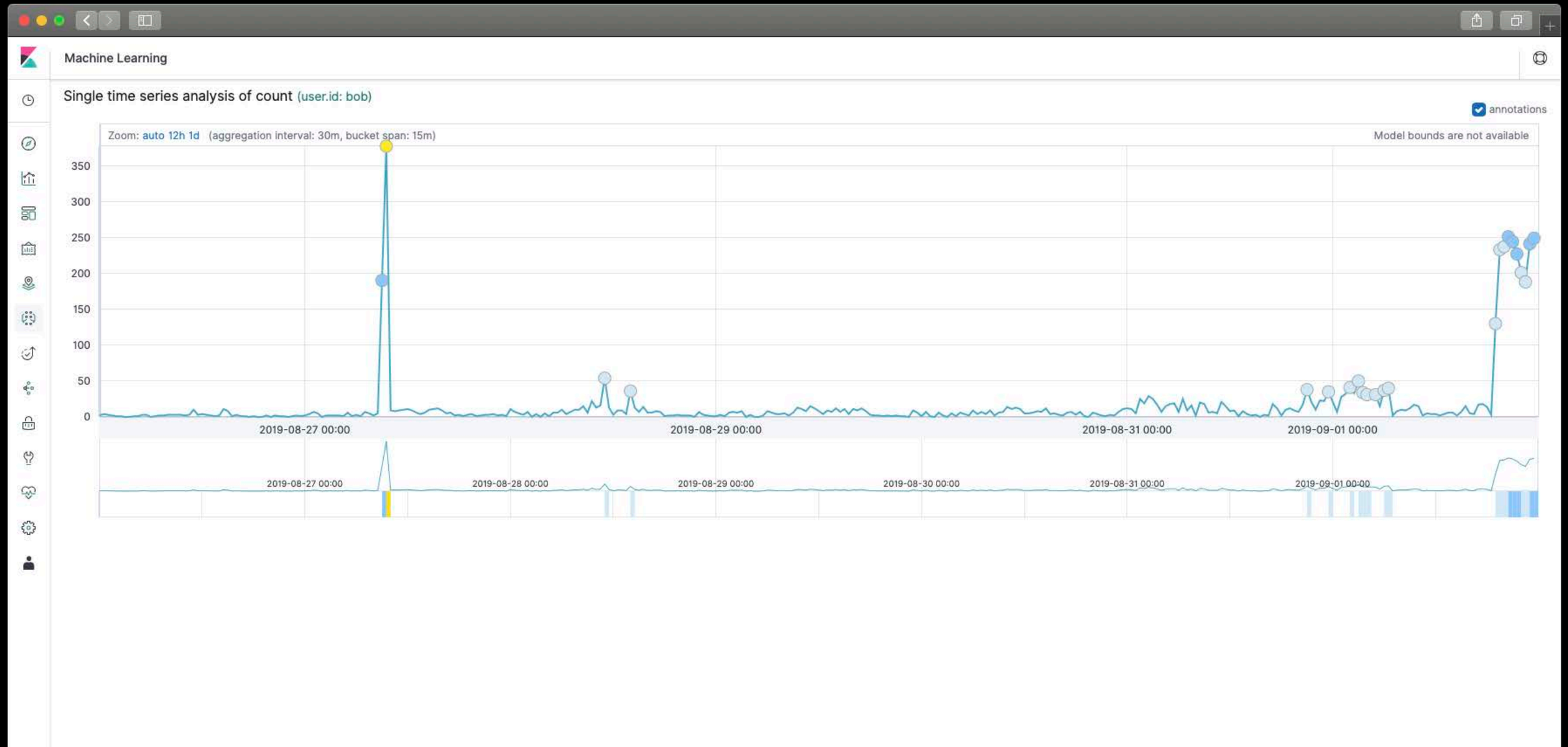


Follow instructions



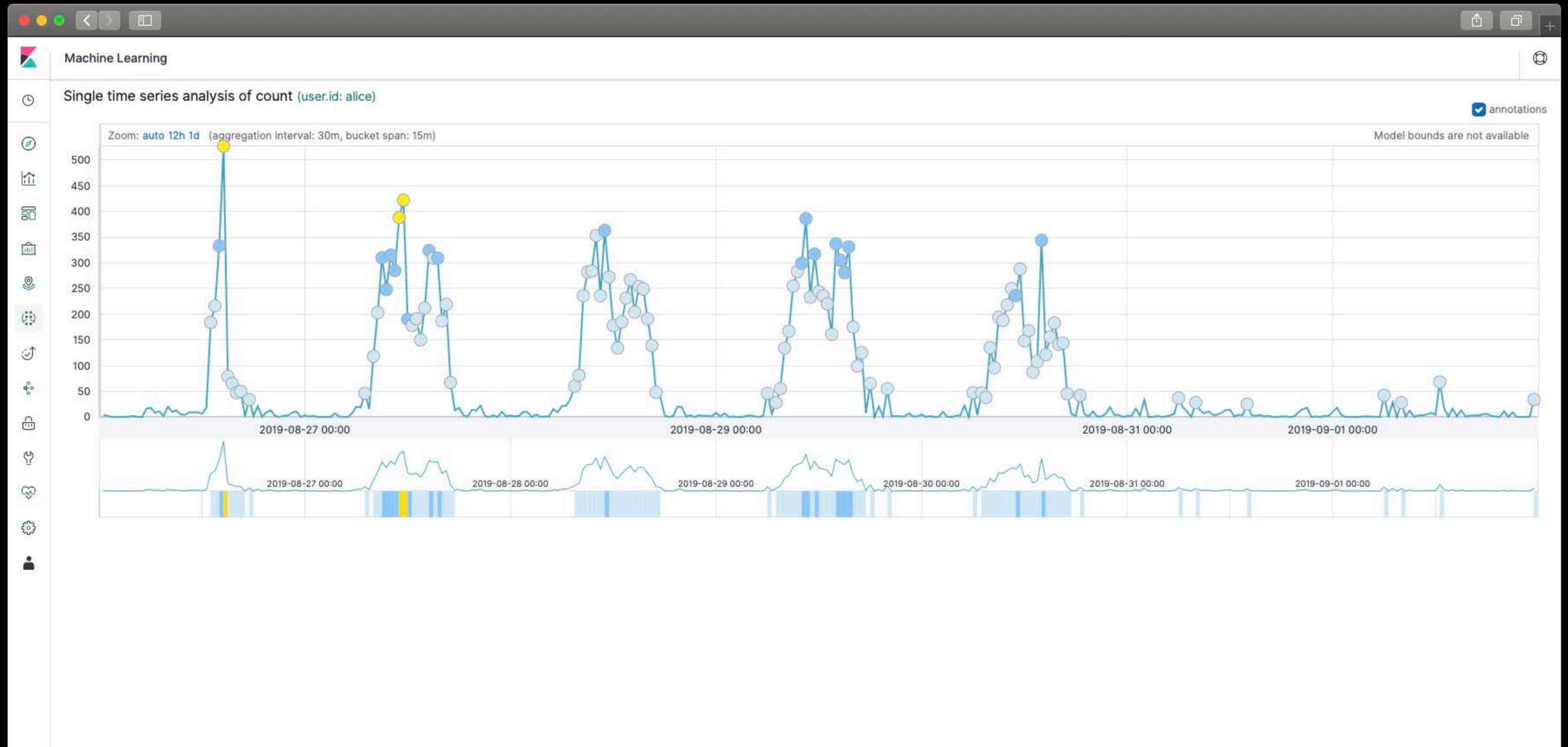
Not All Entities are the Same

UNIVERSITY OF OXFORD



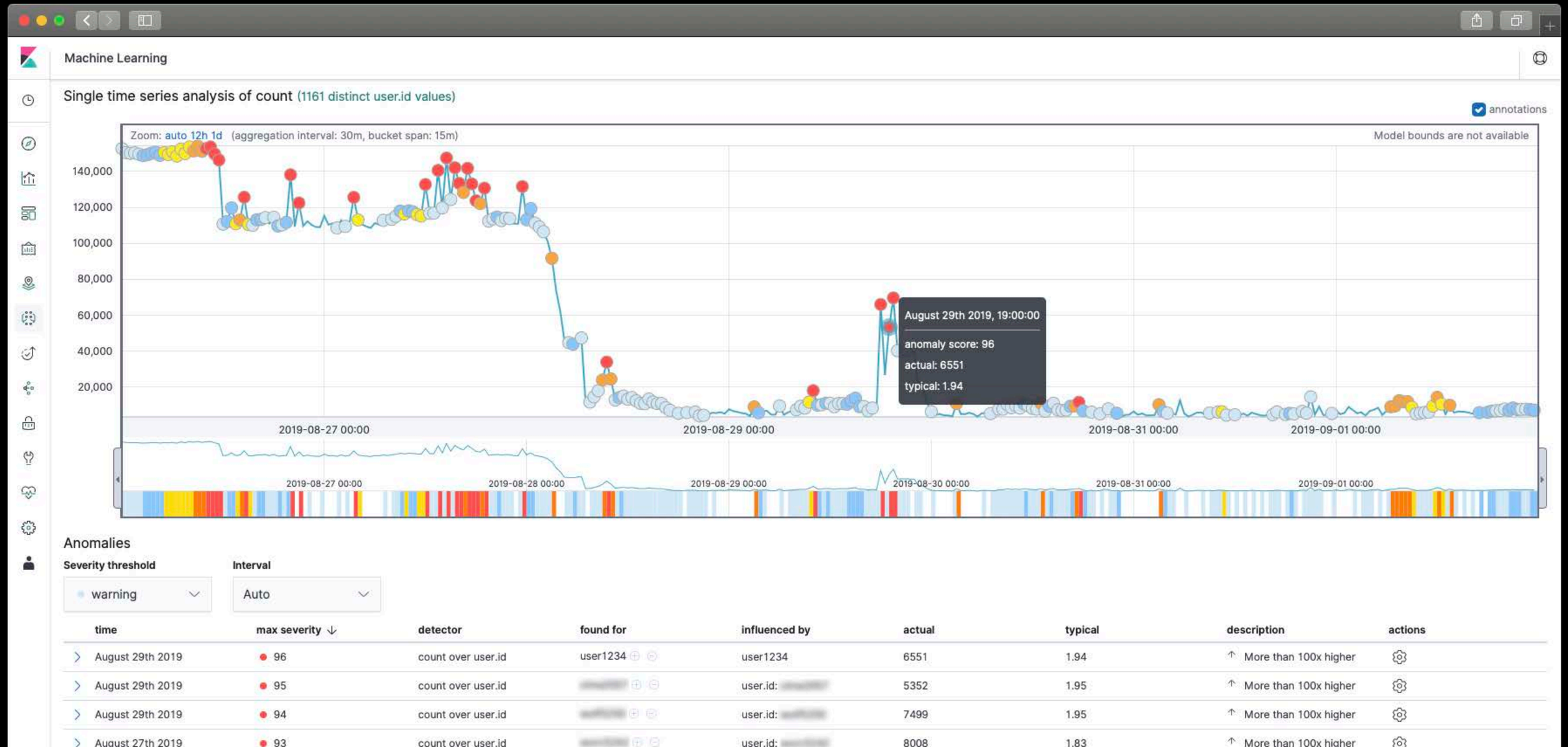
Not All Entities are the Same

UNIVERSITY OF OXFORD



Time Series Analysis

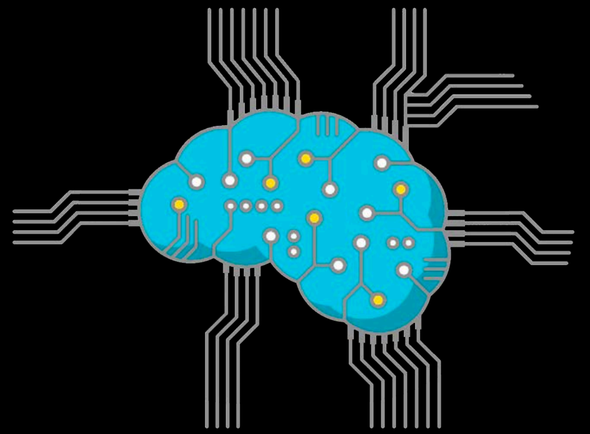
UNIVERSITY OF OXFORD



UNIVERSITY OF OXFORD

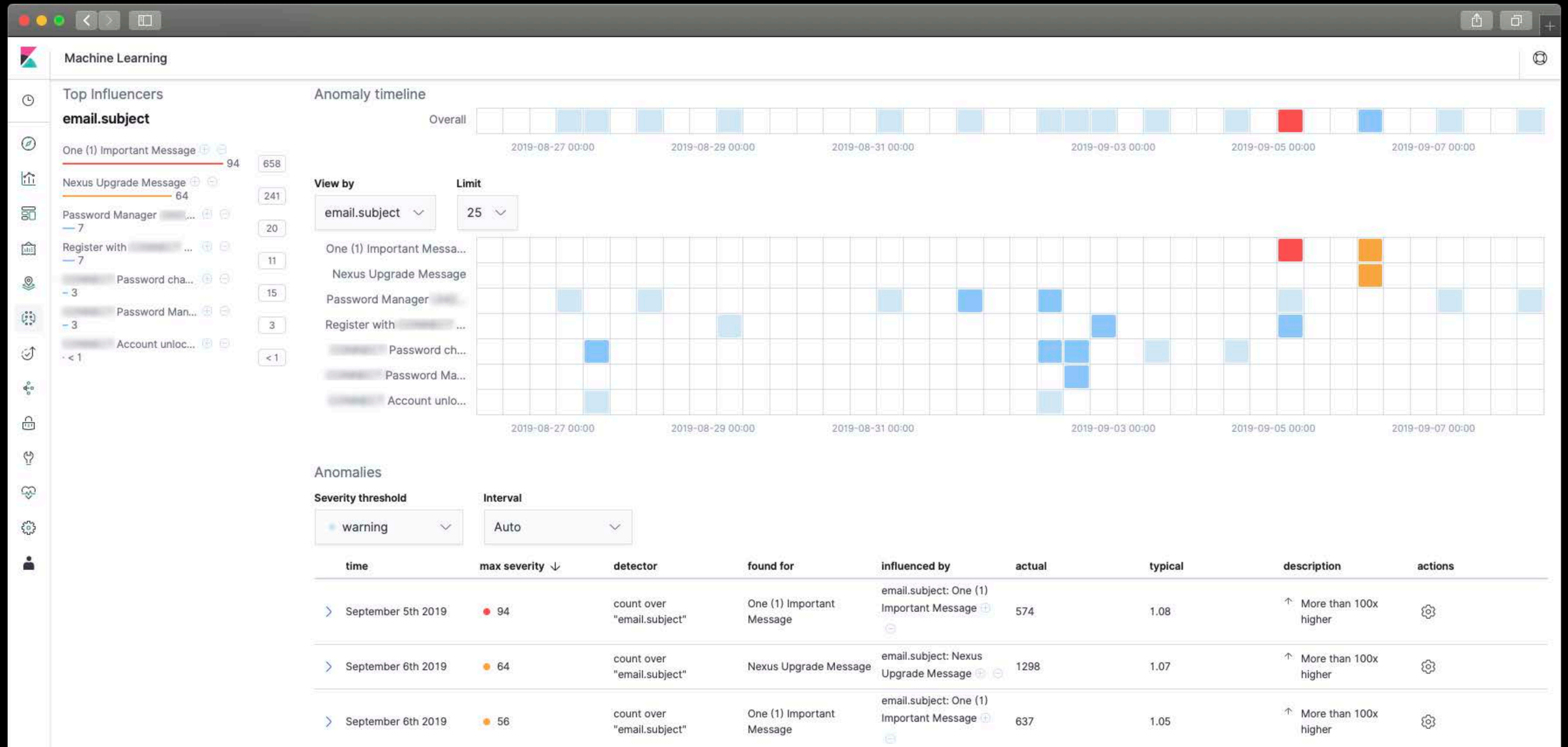
Security Analyst's experience

Unbiased evidence in data



Anomaly Timeline for One Entity

UNIVERSITY OF OXFORD



SIEM+ Got a Little Smarter

UNIVERSITY OF OXFORD

SIEM+

Entity Behaviour Analytics

Data storage

Data aggregation

Data correlation

Security analysis

Alerting

SIRT

UNIVERSITY OF OXFORD

SIEM+

Entity and User Behaviour Analytics ✓

Security Orchestration, Automation and Response

Threat Intel Retro-Matching

Future: Automated Countermeasures

UNIVERSITY OF OXFORD

Not Secure — docs.trendmicro.com/en-us/enterprise/cloud-app-security-integration-api-online-help/supported-cl

Online Help Center

Search

Home / Enterprise / Cloud App Security Integration API Online Help

Privacy and Personal Data Collection Disclosure

Getting Started with Cloud App Security Automation and Integration APIs

Supported Cloud App Security Automation APIs

- Log Retrieval API
- Threat Investigation API
- Threat Mitigation APIs

API Responses

Supported Cloud App Security Automation APIs

This section discusses the following supported Cloud App Security Automation APIs.

API Type	Actions	Description
Log retrieval	Get security logs	Retrieves security event logs of the services that Cloud App Security protects
Threat investigation	Sweep for email messages	Searches email messages in protected mailboxes for those that match meta information search criteria
Threat mitigation	Take actions on user accounts	Takes actions on a batch of specified user accounts
	Take actions on email messages	Takes actions on a batch of specified email messages
	Query action results	Queries the results of actions on specified email messages or user accounts

Log Retrieval API

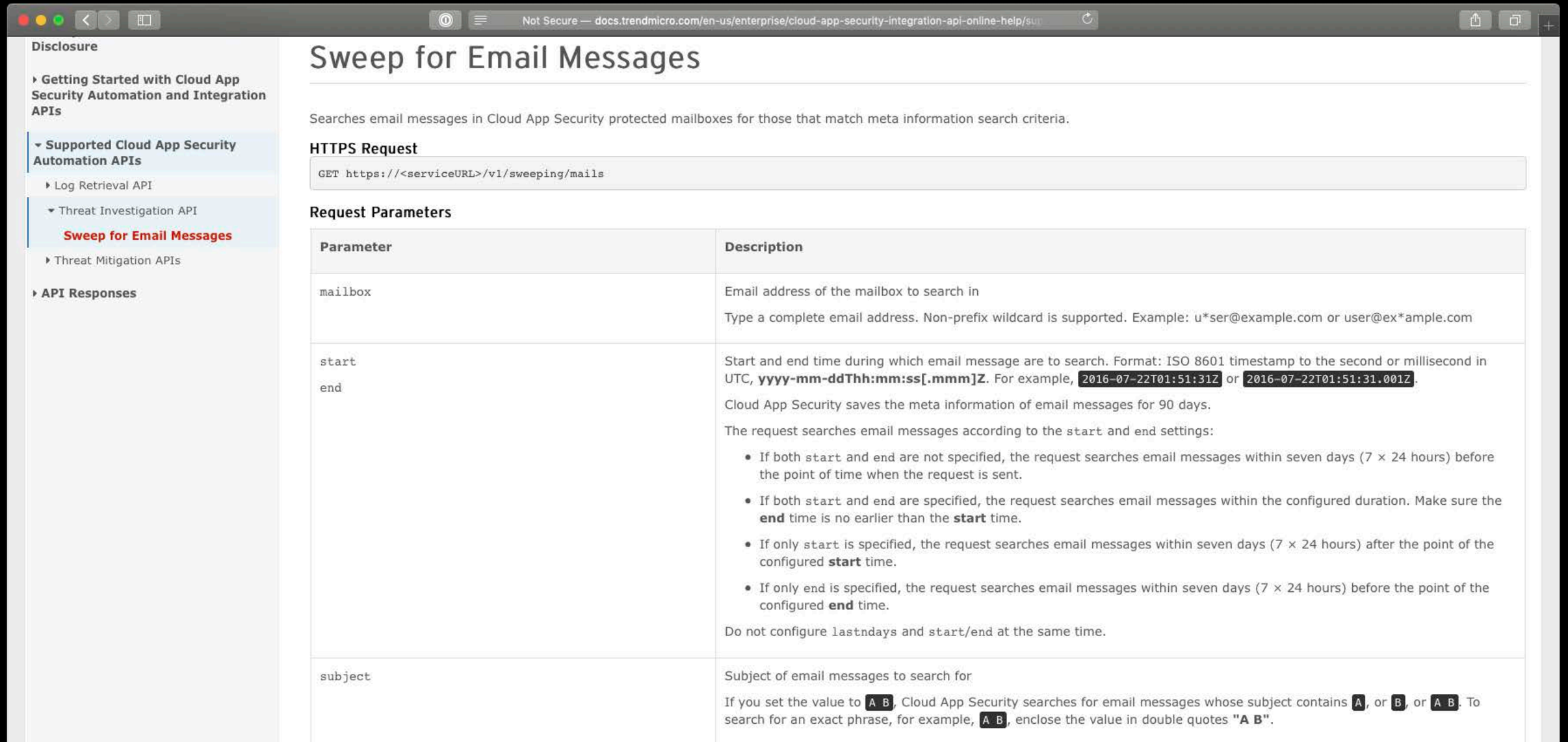
Threat Investigation API

Threat Mitigation APIs

Source: http://docs.trendmicro.com/en-us/enterprise/cloud-app-security-integration-api-online-help/supported-cloud-app-.aspx

Future: Automated Countermeasures

UNIVERSITY OF OXFORD



Proof of Concept Code

UNIVERSITY OF OXFORD

hunting.py

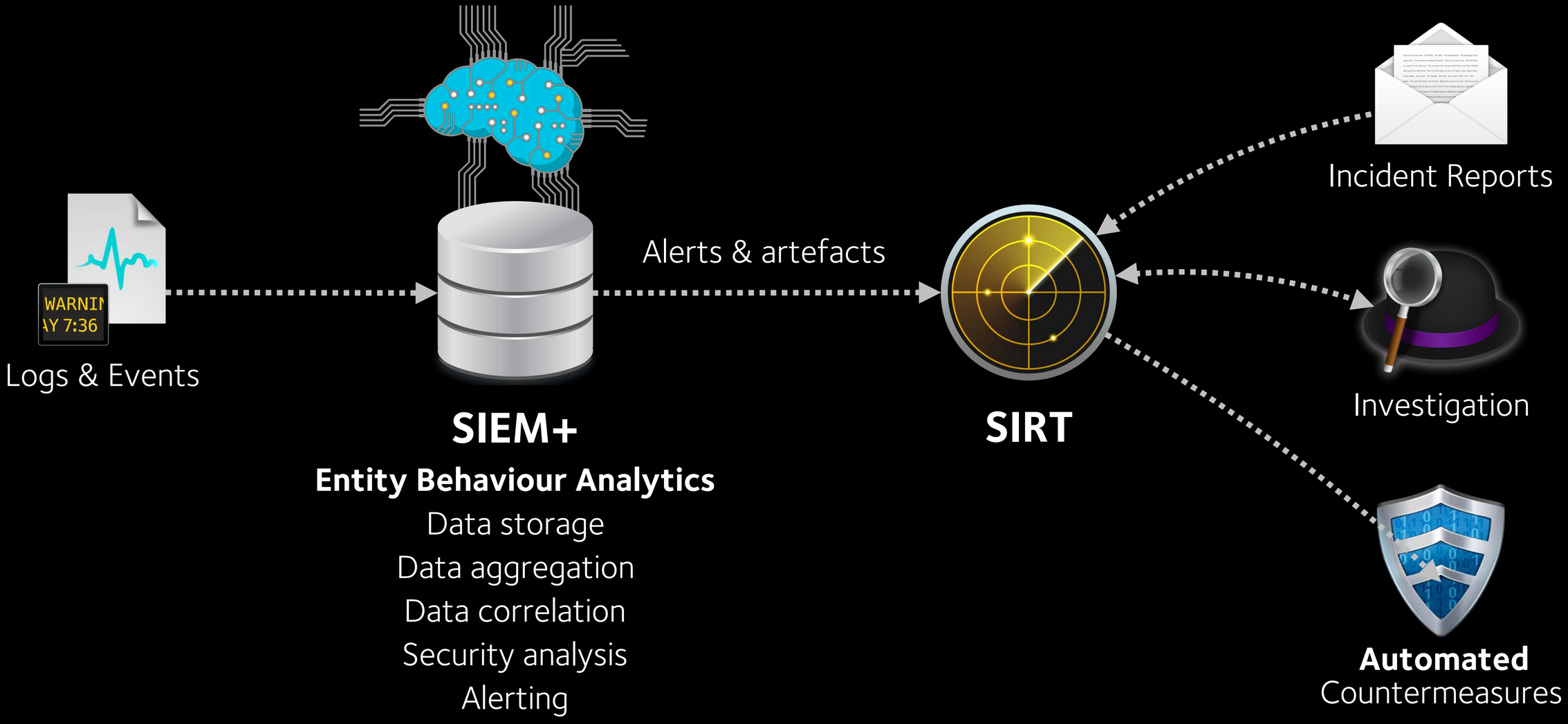
~/Dropbox/publications/2019-09-13 CLOUDSEC Thread Hunting/hunting.py (functions)

```
1  #!/usr/bin/python
2
3  import requests
4
5  session = requests.session()
6  session.headers.update({
7          'Authorization': 'Bearer <secret>' })
8  baseurl = 'https://api-eu.tmcas.trendmicro.com/v1/sweeping/mails'
9
10 params = {}
11 params['limit'] = 500
12 params['start'] = '2019-09-13T00:00:00Z'
13 params['end'] = '2019-09-13T10:00:00Z'
14 params['url'] = 'http://test.acme.com.uk'
15
16 raw_data = session.get(baseurl, params=params)
17 json_data = raw_data.json()
18
19 print "Found: %s" % len(json_data['value'])
20 for v in json_data['value']:
21     print "%s: %s" % ( 'mail_message_subject', v['mail_message_subject'])
22     print "%s: %s" % ( 'mailbox', v['mailbox'])
```

L: 1 C: 18 Python Unicode (UTF-8) Unix (LF) Saved: 12/09/2019, 13:37:57 630 / 70 / 22 100%

SIEM+ Got Even More Smarter

UNIVERSITY OF OXFORD



UNIVERSITY OF OXFORD

SIEM+

Entity and User Behaviour Analytics ✓

Security Orchestration, Automation and Response ✓

Threat Intel Retro-Matching

Data-Driven

Multi-Vendor

APIs

Automation

Big Data

Agility

SecDevOps

Velocity

Permissive Culture

Orchestration

Integration

Adaptability

Retro Matching and Hunting

Thank You!

Aaron Wilson

Linux Security Lead

Marko Jung

Global Head of Information Security Operations

 *m@mju.ng*  *@mjung*  *fb.com/markohjung*